

## VARNOST V SUZP

# Varnost v SUZP

---

- Uporabniki (podatkovne baze):
  - identificirajo se z uporabniškim imenom in geslom.
- Vloge:
  - varnostni mehanizem / optimizacija upravljanja.
- Pravice:
  - uporabnikom dodeljujemo pravice neposredno;
  - uporabnikom dodeljujemo pravice posredno preko vlog.

# SQL DCL

---

- SQL DCL (*ang. Data Control Language*) – primer: MySQL

- Dodajanje uporabniških računov:

```
CREATE USER uporabniško_ime;
```

- Dodajanje vlog:

```
CREATE ROLE naziv_vloge;
```

- Dodeljevanje vlog posameznim uporabnikom:

```
GRANT naziv_vloge TO uporabniško_ime;
```

- Spreminjanje lastnosti uporabniškega računa:

```
ALTER USER uporabniško_ime ...;
```

- Brisanje uporabnika:

```
DROP USER uporabniško_ime;
```

# Gesla

---

## □ Zgradba gesla

- gesla naj ne bi bila „pravilne“ besede;
- gesla naj ne bi bili rojstni dnevi, imena sorodnikov in podobno (nekaj, kar je enostavno povezati z lastnikom);
- gesla so lahko neobičajne kombinacije besed (npr. pes-stol);
- gesla so lahko sestavljena iz črk in številk (npr. luci123);
- gesla naj bodo velika vsaj 8 znakov. Naj bodo težka za uganiti, a enostavna za zapomniti.

## □ Zamenjava gesla:

- gesla je potrebno menjati, vendar ne preveč pogosto.

# Pravice

---

- **SELECT** – omogočene so poizvedbe na tabelah;
- **INSERT** – omogočeno je dodajanje novih zapisov v tabele;
- **UPDATE** – omogočene so spremembe vsebine obstoječih zapisov v tabelah;
- **DELETE** – omogočeno je brisanje zapisov iz tabel;
- **REFERENCES** – omogoča ustvarjanje tujega ključa v podrejenih tabelah;
- **EXECUTE** – omogočeno izvajanje procedur in funkcij;
- **ALTER** – omogočeno spreminjanje strukture tabele;
- **INDEX** – omogočeno ustvarjanje in brisanje indeksov;
- ...

Več v dokumentaciji na spletni strani:

<https://dev.mysql.com/doc/refman/8.0/en/privileges-provided.html>

# Vloge

---

- Namesto neposrednega dodeljevanja posameznih pravic možna uporaba vlog (*angl. roles*)
- Smernice glede uporabe vlog:
  - vlog naj bo čim manj;
  - vloge naj se oblikujejo glede na organizacijske vloge (delovna mesta);
  - uporaba vlog z inkrementalno povečanimi pravicami za edinstvene potrebe, npr.:
    - vloga – vpogled
    - vloga – delo
    - vloga – skrbnik
    - vloga – revizija

# SQL DCL

---

- Dodeljevanje pravic na tabeli uporabniku/vlogi:

```
GRANT pravica ON ime_tabele TO  
ime_uporabnika|ime_vloge;
```

- Odvzemanje pravic uporabniku/vlogi:

```
REVOKE pravica ON ime_tabele FROM  
ime_uporabnika|ime_vloge;
```

# Naloga (1)

---

1. Ustvari naslednje tabele:

T1 ( a INTEGER, b INTEGER );

T2 ( c INTEGER, d INTEGER );

T3 ( e INTEGER, f INTEGER );

T4 ( g INTEGER, h INTEGER );

T5 ( i INTEGER, j INTEGER );

2. Ustvari nove vloge:

vpogled

prodaja

skrbnik

# Naloga (2)

---

3. Priredi naslednje pravice ustreznim vlogam:

Objekt	v pogled	prodaja	skrbnik
T1	S	SUI	SUID
T2	S	SUI	SUID
T3	S	SUI	SUID
T4	S	S	SUID
T5	-	UI	SUI

**S – SELECT, U – UPDATE, I – INSERT, D – DELETE**

# Naloga (3)

---

4. Ustvari naslednje uporabnike in jim dodeli naslednje vloge:

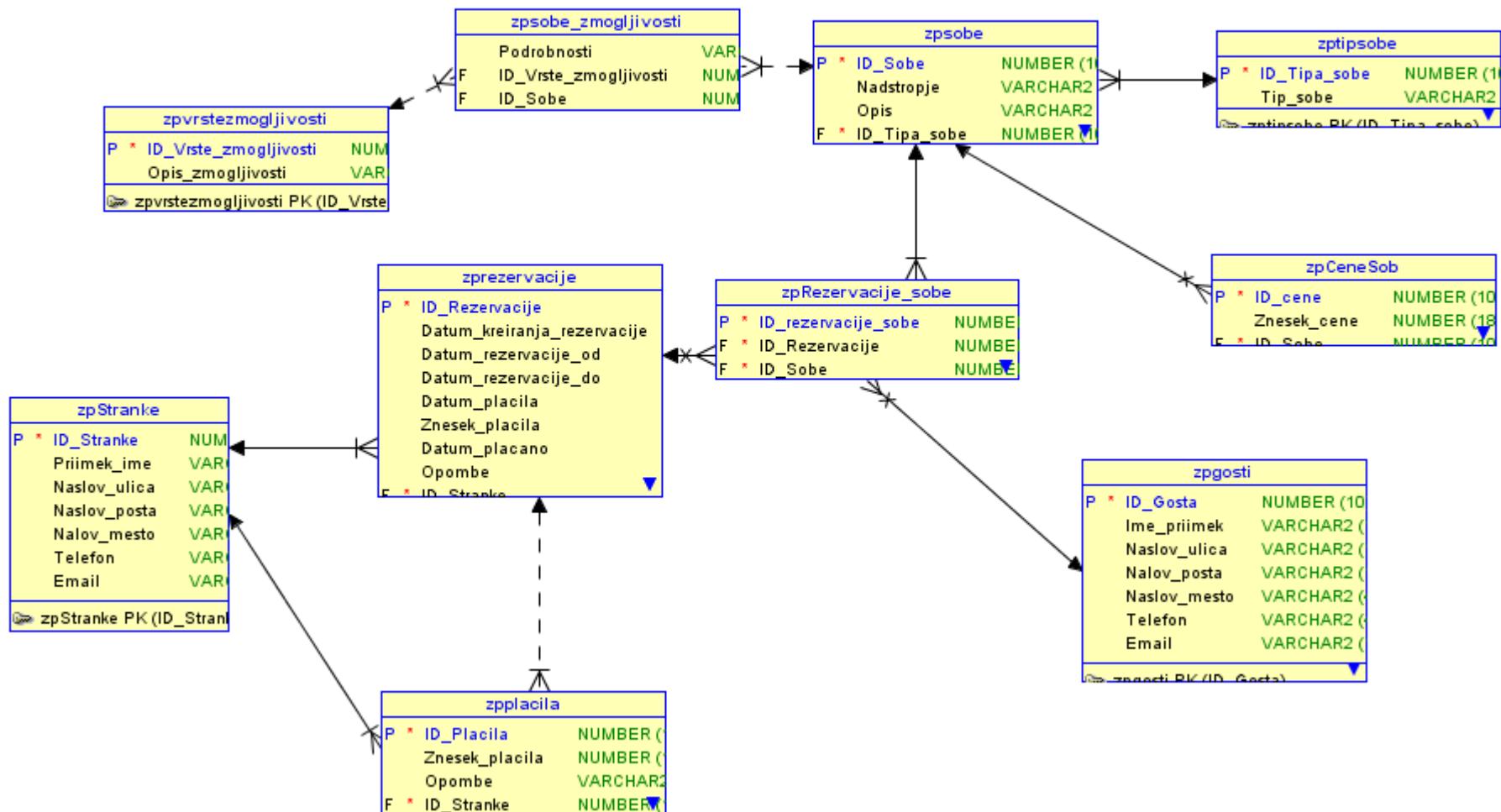
<b>uporabnik</b>	<b>vloge</b>
<b>stanislav</b>	prodaja
<b>vojko</b>	prodaja
<b>snezna</b>	vpogled
<b>zdravko</b>	vpogled
<b>zlata</b>	prodaja, skrbnik
<b>srecko</b>	prodaja, skrbnik
<b>nada</b>	skrbnik
<b>milan</b>	skrbnik

# Naloga (4)

---

5. **Stanislav** je dal odpoved in je zaradi tega potrebno umakniti njegov uporabniški račun.
6. Novo zaposlena je **Milica** za katero je potrebno ustvariti novo uporabniško ime oz. račun. Milica naj ima iste pravice, kot jih je prej imel **Stanislav**.
7. V organizacijo pride revizor in zahteva vpogled v vse podatke sistema. Ustvari vlogo **revizija**, kateri je potrebno dodeliti pravice vpogleda (**SELECT**) v vse tabele. Ustvari novega uporabnika **revizor** in mu dodali vlogo **revizija**.
8. Revizor je ugotovil, da je v sistemu dodeljeno preveč pravic, in sicer vloga **prodaja** ne bi smela imeti možnosti spreminjanja in vnosa v tabelo **T3**. Ustrezno dopolni vlogo **prodaja** in preveri dostope do baznih objektov po spremembji.
9. Odstrani vse vloge (vpogled, prodaja, skrbnik, revizija) in vse uporabnike, ki so bili ustvarjeni v tej nalogi.

# Naloga – hotelski rezervacijski sistem



# Naloga – hotelski rezervacijski sistem

---

1. Ustvarite sistem vlog za hotelski rezervacijski sistem. Vloge naj bodo naslednje:

- stranka** (ki ima možnost pregleda ponudbe, ne sme pa ničesar spremenjati);
- računovodstvo** (ki ima možnost vpogleda, dodajanja in spremnjanja finančnih podatkov-rezervacij);
- recepција** (ki ima možnost vpogleda, dodajanja in spremnjanja vseh podatkov, razen šifrantov – zmoglјivosti sob, cenika in vrst sob);
- direktor** (ki ima možnost vpogleda v vse podatke, ne sme pa ničesar spremenjati);
- skrbnik** (ki ima možnost vpogleda, dodajanja in spremnjanja vseh podatkov).

2. Naredi razpredelnico, v kateri bodo vidne vloge in pravice na tabelah.

3. Dodeli vlogam pravice na ustrezne bazne objekte (tabele).

4. Kreiraj nekaj uporabnikov in jim dodeli eno od vlog.